Sarvaank

Law Decoded for *Entrepreneurs*

ANALYSIS ON DIGITAL PERSONAL DATA PROTECTION RULES 2025

PART-2

In the contemporary digital landscape, data has emerged as a powerful resource, often referred to as being "the new oil". The growing volume of personal data calls for a robust and comprehensive legal framework to address concerns surrounding privacy, security, and ethical data usage.

The Digital Personal Data Protection Rules, 2025, ("**Rules**") represent a vital step in operationalizing the framework established by the Digital Personal Data Protection Act, 2023 ("**Act**"). Together, they aim to create a structured and accountable environment for data protection in India, addressing the growing challenges of digital privacy and security.

In Part I of this series, the historical evolution of data protection in India was explored, highlighting the recognition of privacy as a fundamental right through landmark judgments like *Puttaswamy*[1] and the principles governing Data Fiduciaries and Data Principals under the Act. While the meaning and obligations of Data Fiduciaries and Data Principals form the bedrock of the Act. Consent Managers, the imposition of penalties for non-compliance, the establishment of the Data Protection Board of India, and other key elements are an essential component of the Rules which will be detailed herein.

Consent Managers

The Rules place significant emphasis on the role of Consent Managers. These entities are pivotal in facilitating Data Principals *(as discussed in Part 1)*—the individuals to whom the data pertains—in managing their consent for personal data processing.

The Act defines Consent Managers as a person registered with the Data Protection Board of India ("**Board**") who acts as a single point of contact to enable Data Principals to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform.[2]

Registration and Obligations of Consent Managers: [3]

An entity fulfilling the conditions for registration of Consent Managers as specified below, may apply to the Board by furnishing required particulars and documents. The Board, upon receipt of the application, may conduct inquiries to assess compliance with these conditions. If satisfied, it will register the applicant as a Consent Manager and publish their particulars on its website. If not, it will reject the application, providing reasons for the rejection.

If the Board identifies non-adherence to conditions and obligations, it may, after giving the Consent Manager an opportunity to be heard, direct compliance measures. In cases of persistent violations, the Board may suspend or cancel the registration to protect the interests of Data Principals, recording reasons in writing. The Board may also require the Consent Manager to furnish additional information as needed for the purpose of ensuring compliance.

Conditions of Registration of Consent Manager[4]:

Criteria	Requirement
Eligibility	The applicant must be a company incorporated in India.

[1] Supreme Court, Writ Petition (Civil) No 494 Of 2012.
[2] Section 2(g), Digital Data Protection Act, 2023.
[3] Rule 4, Digital Data Protection Rules, 2025 (Draft), *3rd January 2025*
[4] Part A, First Schedule, Digital Data Protection Rules, 2025 (Draft), *3rd January 2025*

Conditions	The applicant must have adequate technical, operational, and financial capacity to fulfill its obligations as a Consent Manager. The applicant's financial condition and management must be sound.
New Worth	The applicant must have a net worth not less than Rs. 2 Crores.
Business Viability	The applicant's volume of business, capital structure, and earning prospects must be adequate.
Integrity of Management	Directors, key managerial personnel, and senior management must have a general reputation and record of fairness and integrity.
Governing Documents	The memorandum of association and articles of association must include provisions requiring adherence to obligations in Part B, with policies and procedures in place to ensure compliance. Amendments to these provisions require prior approval from the Board.

Obligations of Consent Manager[5]

1. The Consent Manager shall enable a Data Principal to give consent for the processing of its personal data to a Data Fiduciary onboarded onto the platform, either directly to such Data Fiduciary or through another Data Fiduciary maintaining such data.

2. It shall ensure that the manner in which personal data is shared or made available is such that its contents are not readable by the Consent Manager itself.

3. The Consent Manager is required to maintain a record of consents given, denied, or withdrawn by Data Principals, notices accompanying or preceding consent requests, and instances of sharing personal data with transferee Data Fiduciaries. It must also provide

4. Consent Manager shall give the Data Principal, access to the records through its platform and furnish such information in a machine-readable format upon request. These records must be retained for at least seven years or longer, as agreed with the Data Principal or as required by law.

5. Consent Manager shall develop and maintain a website or app, or both, as the primary means for Data Principals to access its services. It is prohibited from subcontracting or assigning its obligations under the Act and Rules. The Consent Manager must take reasonable security measures to prevent personal data breaches and act in a fiduciary capacity in relation to Data Principals.

6. Consent Manager must ensure that no conflicts arise with Data Fiduciaries, including their promoters, key managerial personnel, or senior management. Measures must also be implemented to prevent conflicts of interest due to directors, key managerial personnel, or senior management holding directorships, financial interests, or employment in Data Fiduciaries.

7. The Consent Manager must publish information on its website or app regarding its promoters, directors, key managerial personnel, senior management, shareholders holding more than 2% of its shares, and any other details directed by the Board for transparency.

[5] Part B, First Schedule, Digital Data Protection Rules, 2025 (Draft), *3rd January 2025.*

8. Effective audit mechanisms must be implemented to monitor, evaluate, and report compliance to the Board periodically or as directed, with respect to technical and organizational controls, systems, procedures and safeguard, continued fulfilments of the condition of registration and adherence under the Act and these Rules.

9. The company registered as Consent Manager shall not be transferred by sale, merger or otherwise, except by obtaining a prior approval of the Board, fulfilling such conditions as may be specified by the Board.

10. The Consent Manager must maintain a mechanism to redress grievances of Data Principals regarding their rights under the Act and publish information about its grievance redressal process on its platform[6].

Processing of Personal Data Outside India

Recognizing the need to safeguard the rights of individuals while addressing international data transfers, Act and the Rules incorporates provisions governing the processing of personal data outside India.

The Central Government is empowered to restrict the transfer of personal data by a Data Fiduciary to any country or territory outside India through a notification. Such restrictions will not affect the applicability of any other Indian laws that provide a higher degree of protection or impose stricter conditions for the transfer of personal data outside India.[7]

Further, as per the Rules, transfer of personal data to any country or territory outside India by a Data Fiduciary is subjected to certain restrictions, with respect to:

1. Personal data processed by a Data Fiduciary within the territory of India, and
2. Personal data processed outside the territory of India in connection with any activity related to the offering of goods or services to Data Principals within the territory of India.[8]

This transfer is permitted only if the Data Fiduciary complies with the requirements specified by the Central Government. These requirements may be issued through general or special orders and will govern the availability of such personal data to any foreign State, or any person, entity, or agency under the control of such a State.

General Exemptions Under the Act[9]

Exemptions	Description
Exemptions for Specific Processing Needs	Provisions of Chapter II (*Obligations of Data Fiduciaries*, except for subsections *8(1) and 8(5)),* Chapter III (*Rights and Duties of Data Principals*), and Section 16 (*Processing of Personal Data Outside India*) do not apply in cases where: **(a)** Processing of personal data is necessary to enforce any legal right or claim.

[6] Rule 13(3), Digital Data Protection Rules, 2025 (Draft), *3rd January 2025.*
[7] Section 16, Digital Data Protection Act, 2023.
[8] Rule 14, Digital Data Protection Rules, 2025 (Draft), *3rd January 2025.*
[9] Section 17, Digital Data Protection Act, 2023.

	(b) Processing of personal data by courts, tribunals, any other body entrusted by law in India with judicial, quasi-judicial, regulatory, or supervisory functions, where such processing is necessary for the performance of these functions. **(c)** Personal data is processed for prevention, detection, investigation, prosecution of offence or contraventions of any law in force in India. **(d)** Processing of personal data of Data principal who is not located in India if such processing is pursuant to a contract entered with any person outside India by a person based in India. **(e)** Processing of personal data is necessary for scheme of compromise or arrangement, merger or amalgamation, demerger, reconstruction, or transfer of undertakings of companies, provided the process is approved by a competent court, tribunal, or authority under applicable laws. **(f)** Processing is necessary for ascertaining the financial information, assets, and liabilities of individuals who have defaulted on loans or advances taken from financial institutions, subject to compliance with applicable laws governing information disclosure.
Broader Exemptions for Certain State Activities and Research	The provisions of the Act do not apply when: **(a)** Processing of personal data is in the interest of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offence relating to any of these. **(b)** Any necessary research, archiving, Statistical purposes, provided the personal data is not used to make decisions affecting specific individuals and adheres to prescribed standards.
Exemptions for Specific Data Fiduciaries	The Central Government may notify certain Data Fiduciaries or classes of Data Fiduciaries, including startups, as exempt from the following provisions: **(a)** Section 5: Notice requirements for obtaining consent. **(b)** Subsections 8(3) and 8(7): Completeness, accuracy, and retention-related obligations. **(c)** Sections 10 and 11: Additional obligations for Significant Data Fiduciaries and access to information by Data Principals.
Processing by State Instrumentalities	For state or any of its instrumentalities, the following provisions are inapplicable: **(a)** Subsection 8(7): Obligations related to erasure of personal data. **(b)** Subsection 12(3): Rights of Data Principals concerning correction and erasure, provided the processing does not involve decisions affecting individuals.
Temporary Exemptions	The Central Government may, before the expiry of five years from the commencement of the Act, notify specific exemptions for certain Data Fiduciaries or classes of Data Fiduciaries for specified periods.

Data Protection Board of India

The Board serves as a pivotal institution to address concerns related to data security, privacy, and accountability, safeguarding the rights of individuals while maintaining a balance between innovation and regulation. The Board's establishment is driven by the need to mitigate risks associated with data breaches, oversee compliance with data protection laws, and provide a structured redressal mechanism for grievances. Its purpose is to enforce transparency, ensure ethical data handling, and uphold the principles of natural justice through fair and timely adjudication.

Section	Provision	Details
18	Establishment of the Board	The Board is established by notification of the Central Government. It is a corporate body with perpetual succession and a common seal, with power to sue or be sued, acquire, hold, and dispose of property. Its headquarters will be notified by the Government.
19	Constitution of the Board	The Board comprises a Chairperson and Members appointed by the Central Government. Appointees must possess ability, integrity, and expertise in relevant fields, with at least one member being an expert in law.
20	Terms of Office	Chairperson and Members serve a 2 (two) year term and are eligible for reappointment. Salaries and terms cannot be altered to their disadvantage after appointment.
21	Disqualifications and Removal	Grounds for disqualification for Chairperson or Member include insolvency, conviction for moral turpitude, incapacity, financial interest affecting impartiality, or abuse of position. Removal requires an opportunity for the Member to be heard.
22	Resignation and Filling of Vacancies	Members may resign by written notice. Vacancies due to resignation, removal, or death are to be filled through fresh appointments as per the Act. Post-tenure employment restrictions apply, subject to the approval by Central Government.
23	Procedures of the Board	Meetings may be held digitally, and procedures are prescribed. Proceedings of the Board are valid even in cases when: (i) there is a vacancy or an issue with how the Board is formed, (ii) issue regarding appointment of a person as Chairperson or another Member or (iii) a procedural irregularity that doesn't affect the substance or outcome of the decision. The Senior-most Member acts as Chairperson during the latter's absence.
24	Appointment of Officers and Employees	The Board may appoint officers and employees as deemed necessary for its functioning, with Central Government approval. Terms of service are to be prescribed.
25	Status as Public Servants	Chairperson, Members, officers, and employees are deemed public servants under Section 2(28) of Bhartiya Nyaya Sanhita, 2023.

26	Powers of the Chairperson	Chairperson oversees administrative matters, authorizes officers for scrutiny, and allocates proceedings among Members or groups of Members.

Search-cum-Selection Committee

The Central Government forms a Search-cum-Selection Committee to recommend candidates for appointment to the Board. For appointing the Chairperson, the Committee is chaired by the Cabinet Secretary and includes the Secretaries from the Department of Legal Affairs and the Ministry of Electronics and Information Technology, along with 2 (two) experts with relevant expertise. For Members other than the Chairperson, the Committee is chaired by the Secretary of the Ministry of Electronics and Information Technology and includes the Secretary of Legal Affairs and two experts of repute. The Government considers these recommendations and appoints suitable candidates. Proceedings of the Committee cannot be challenged due to vacancies or procedural defects[10].

Powers, Functions and Procedures to be followed by the Board[11]

Section	Provision	Power/Function
27(1)(a)	Action on personal data breach	Upon receiving information about any breach of personal data, the Board can direct urgent remedial or mitigation measures. It can also inquire into the breach and impose penalties as prescribed under the Act.
27(1)(b)	Complaints by Data Principals	The Board can act on complaints about breaches by Data Fiduciaries, violations of obligations related to personal data, or exercise of rights. It may also respond to government references or court directions, inquire into such breaches, and impose penalties.
27(1)(c)	Breach by Consent Manager	The Board addresses complaints regarding Consent Managers failing to meet their obligations related to personal data and imposes penalties for such breaches.
27(1)(d)	Breach of registration conditions	When notified of a breach of registration conditions by a Consent Manager, the Board conducts an inquiry and imposes penalties where necessary.
27(1)(e)	Breaches by intermediaries	For breaches by intermediaries under Section 37(2) of the Act, the Board acts upon references from the Central Government to inquire into the matter and impose penalties.
27(2)	Issuance of directions	The Board may issue binding directions to concerned persons after hearing them and recording written reasons.
27(3)	Review of directions	Directions issued under Section 27(1) or (2) of the Act can be modified, suspended, withdrawn, or canceled by the Board based on representations by affected persons or government references. Conditions may be imposed for such changes.

[10] Rule 16, Digital Personal Data Protection Rules (Draft), *3rd January, 2025*
[11] Chapter VI, Digital Personal Data Protection Act, 2023

28(1)	Digital operations	The Board functions as an independent digital entity, leveraging technology for the receipt of complaints, hearings, and decision-making processes, adopting prescribed techno-legal measures.
28(2)	Response to complaints or references	The Board is empowered to act on complaints, references, or directions as specified in Section 27(1) of the Act, following the Rules and provisions of the Act.
28(3)	Grounds for inquiry	The Board determines whether sufficient grounds exist to initiate an inquiry into a matter.
28(4)	Closure of proceedings	If insufficient grounds are found, the Board may close the proceedings, provided the reasons are recorded in writing.
28(5)	Initiation of inquiry	If sufficient grounds exist, the Board conducts an inquiry into the person's affairs to ensure compliance with the provisions of the Act, recording reasons in writing.
28(6)	Principles of natural justice	All inquiries are conducted following principles of natural justice, with reasons for actions documented throughout the process.
28(7)	Powers akin to a civil court	The Board has powers similar to a civil court, including summoning individuals, receiving evidence, requiring document discovery, inspecting data, and performing other prescribed functions under the Code of Civil Procedure, 1908.
28(8)	Limitation on access	The Board or its officers are not in any position to prevent access to premises or taking custody of items that may disrupt an individual's or entity's day-to-day functioning.
28(9)	Assistance from authorities	The Board may request assistance from police or government officers, who are obligated to comply with such requests.
28(10)	Interim orders	During an inquiry, the Board may issue interim orders after providing the concerned party an opportunity to be heard and recording reasons in writing.
28(11)	Conclusion of inquiry	After conducting an inquiry, the Board may either close the proceedings or impose a monetary penalty for significant breaches of the Act, considering factors such as severity, impact, repetition, mitigation efforts, proportionality, and potential consequences for the offender, while ensuring the concerned party is heard and reasons are recorded.
28(12)	False or frivolous complaints	If a complaint is found to be false or frivolous, the Board can issue warnings or impose costs on the complainant.

Power of Central Government to Issue Directions[12]

The Central Government, or any authorized officer, can block access to certain information related to a Data Fiduciary if: (i) the Board informs the government in writing that the Data Fiduciary has been penalized at least twice for violation, (ii) blocking the information is deemed necessary for the public's interest. Before taking such action, the Data Fiduciary must be given an opportunity to be heard, and the government must clearly state the reasons for the decision in writing. Once the government issues the blocking order, any organization or intermediary receiving the directive must comply with it.

The terms "computer resource," "information," and "intermediary" have the same meanings as defined in the Information Technology Act, 2000.

Meetings and Decision-Making of the Board

The Chairperson organizes Board meetings, sets the agenda, and issues notices. Meetings are chaired by the Chairperson. or, in her absence, a Member chosen by attendees. Decisions require a one-third quorum and are made by majority vote, with the Chairperson having a casting vote in case of a tie. Members with conflicts of interest abstain from participation. In emergencies, the Chairperson can act independently which shall be informed to the Members within 7 (seven) days for ratification. Items may also be decided through circulation with majority approval. All orders and decisions are formally authenticated[13].

Inquiry Timeframes

The Board must complete inquiries within 6 (six) months of receiving a complaint, reference, or direction under Section 27 of the Act. Extensions of up to 3 (three) months can be granted if reasons are recorded in writing, ensuring timely yet thorough resolutions[14].

Digital Functioning of the Board

The Board functions as a digital office, using technology to minimize physical presence during proceedings. It retains the authority to summon and examine individuals while ensuring efficient and transparent digital operations through techno-legal measures[15].

Voluntary Undertaking[16]:

Further, the Data Protection Board is empowered to accept a voluntary undertaking from any individual or entity at any stage of proceedings initiated under Section 28 of the Act. The undertaking must pertain to matters connected with the compliance or observance of the Act's provisions. The voluntary undertaking may contain specific commitments by the individual or entity giving the undertaking. These commitments could include undertaking certain actions within a time frame determined by the Board, refraining from specified actions to ensure compliance, publicizing the undertaking.

[12] Section 37, Digital Personal Data Protection Act, 2023
[13] Rule 18, Digital Personal Data Protection Rules (Draft), *3rd January, 2025*
[14] Rule 18(9), Digital Personal Data Protection Rules (Draft), *3rd January, 2025*
[15] Rule 19, Digital Personal Data Protection Rules (Draft), *3rd January, 2025*
[16] Section 32, Digital Personal Data Protection, Act, 2023.

Once the Board accepts a voluntary undertaking, it may vary the terms with the consent of the person giving such undertaking, and after acceptance, the Board shall constitute a bar on proceedings under the provisions of the Act.

If the individual fails to comply with any term of the voluntary undertaking, such non-compliance will be treated as a breach of the Act's provisions. In such cases, the Board may take appropriate action under Section 33 of the Act, following the principles of natural justice by providing the person with an opportunity to be heard.

Appeal and Alternate Dispute Resolutions

The Act provides a mechanism for individuals or entities aggrieved by an order or direction of the Data Protection Board of India to file an appeal before the Appellate Tribunal ("**Tribunal**"). Key features include[17]:

(a) The appeal must be filed **within 60 days** from the date of receipt of the order or direction.

(b) The Tribunal may entertain appeals beyond the prescribed period if sufficient cause is shown.

(c) After hearing the parties, the Tribunal may confirm, modify, or set aside the order appealed against.

(d) The Tribunal shall send a copy of every order made by it to the Board and to the parties to the appeal.

(e) The Tribunal is required to dispose of appeals expeditiously, aiming to conclude proceedings within six months. Failing to dispose of within six months, the Tribunal shall record its reasons in writing for not disposing the appeal within that period.

Further, the orders passed by the Tribunal under the Act are executable as a decree of a civil court. The Tribunal can enforce its orders directly or transmit them to a civil court with jurisdiction for execution.[18] The Act also permits the Data Protection Board to direct parties to resolve disputes through mediation. Mediation must involve a mutually agreed-upon mediator or follow provisions under applicable laws.[19]

Penalties and Adjudications[20]:

Description	Penalty
Breach of the obligation by a Data Fiduciary to implement reasonable security safeguards for preventing personal data breaches, which compromises the protection of personal data.[21]	May extend to two hundred and fifty crore rupees
Failure to provide notification of a personal data breach to the Data Protection Board of India and affected Data Principals within the prescribed time and manner.[22]	May extend to two hundred crore rupees

[17] Section 29, Digital Personal Data Protection, Act, 2023.
[18] Section 30, Digital Personal Data Protection, Act, 2023.
[19] Section 31, Digital Personal Data Protection, Act, 2023.
[20] The Schedule, Digital Personal Data Protection Act, 2023.
[21] Section 8(5), Digital Personal Data Protection Act, 2023.
[22] Section 8(6), Digital Personal Data Protection Act, 2023.

Breach of obligations regarding the processing of children's personal data, including obtaining verifiable consent from parents or lawful guardians and avoiding harmful processing activities like profiling.[23]	May extend to two hundred crore rupees
Breach of additional obligations imposed on Significant Data Fiduciaries, including appointing a Data Protection Officer, conducting data audits, or completing a Data Protection Impact Assessment.[24]	May extend to one hundred and fifty crore rupees
Breach of duties imposed on Data Principals, such as providing false information, suppressing material details, or filing frivolous complaints or grievances under the Act.[25]	May extend to ten thousand rupees.
Violation of terms in a voluntary undertaking agreed upon with the Data Protection Board during the course of proceedings under the Act.[26]	Up to the extent applicable for the breach.
Breach of any other provision of the Act or rules made thereunder, which do not fall within the specific categories detailed above.	May extend to fifty crore rupees.

Conclusion

The Digital Personal Data Protection Rules, 2025, represent a significant stride in safeguarding privacy and ensuring ethical data practices in the digital era. By outlining clear roles, responsibilities, and frameworks for Consent Managers, Data Fiduciaries, and Data Principals, the Rules complement the foundational Act of 2023, creating a robust data protection ecosystem.

The emphasis on transparency, accountability, and compliance reflects India's commitment to aligning with global standards while addressing domestic challenges. As the digital landscape continues to evolve, these provisions serve as a cornerstone for protecting personal data, fostering trust, and promoting innovation.

****

For more information visit www.sarvaankassociates.com

[23] Section 9, Digital Personal Data Protection Act, 2023.
[24] Section 10, Digital Personal Data Protection Act, 2023.
[25] Section 15, Digital Personal Data Protection Act, 2023.
[26] Section 32, Digital Personal Data Protection Act, 2023.